Research in Cloud Security and Privacy
--Security and Privacy Issues in Cloud Computing

Portions of this PPT draw from PPTs authored by Bharat Bhargava, Anya Kim and YounSun Cho

ASU ARIZONA STATE UNIVERSITY

Outline

- Part I: Introduction
- Part II. Security and Privacy Issues in Cloud Computing

2

Part I. Introduction

- Why do you still hesitate to use cloud computing?
- Causes of Problems Associated with Cloud Computing
- Taxonomy of Fear
- Threat Model

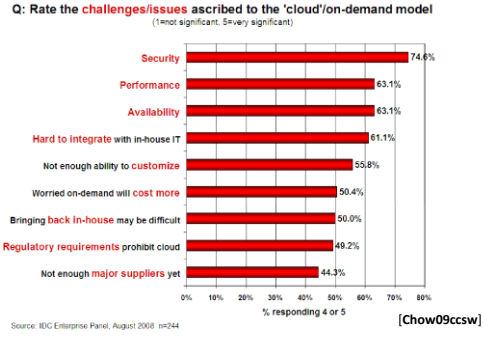
3

Cloud computing is great, why isn't everyone doing it?

- The cloud acts as a big black box, nothing inside the cloud is visible to the clients
- Clients have no idea or control over what happens inside a cloud
- Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity
- Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

4

Companies are still afraid to use clouds



5

Causes of Problems Associated

- Most security problems stem from:
  - Loss of control
  - Lack of trust (mechanisms)
  - Multi-tenancy
- These problems exist mainly in 3rd party management models
  - Self-managed clouds still have security issues, but not related to above

6

Loss of Control in the Cloud

- Consumer's loss of control
  - Data, applications, resources are located with provider
  - User identity management is handled by the cloud
  - User access control rules, security policies and enforcement are managed by the cloud provider
  - Consumer relies on provider to ensure
    - Data security and privacy
    - Resource availability
    - Monitoring and repairing of services/resources

7

Lack of Trust in the Cloud

- A brief deviation from the talk
  - (But still related)
  - Trusting a third party requires taking risks
- Defining trust and risk
  - Opposite sides of the same coin (J. Camp)
  - People only trust when it pays (Economist's view)
  - Need for trust arises only in risky situations
- Defunct third party management schemes
  - Hard to balance trust and risk
  - e.g. Key Escrow (Clipper chip)
  - Is the cloud headed toward the same path?

8

Multi-tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and 'play nicely' ?
  - If they can't, can we isolate them?
- How to provide separation between tenants?

- Cloud Computing brings new threats
  - Multiple independent users share the same physical infrastructure
  - Thus an attacker can legitimately be in the same physical machine as the target

9

Taxonomy of Fear

- Confidentiality
  - Fear of loss of control over data
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromises leak confidential client data
  - Will the cloud provider itself be honest and won't peek into the data?
- Integrity
  - How do I know that the cloud provider is doing the computations correctly?
  - How do I ensure that the cloud provider really stored my data without tampering with it?

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

10

Taxonomy of Fear (cont.)

- Availability
  - Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
  - What happens if cloud provider goes out of business?
  - Would cloud scale well-enough?
  - Often-voiced concern
    - Although cloud providers argue their downtime compares well with cloud user's own data centers

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

11

Taxonomy of Fear (cont.)

- Privacy issues raised via massive data mining
  - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Increased attack surface
  - Entity outside the organization now stores and computes data, and so
  - Attackers can now target the communication link between cloud provider and client
  - Cloud provider employees can be phished

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

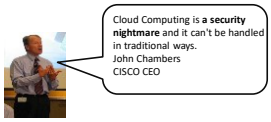
12

Taxonomy of Fear (cont.)

- Auditability and forensics (out of control of data)
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don't maintain data locally
- Legal quagmire and transitive trust issues
  - Who is responsible for complying with regulations?
    - e.g., SOX, HIPAA, GLBA ?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)



- Security is one of the most difficult task to implement in cloud computing.
  - Different forms of attacks in the application side and in the hardware components
- Attacks with catastrophic effects only needs one security flaw

(http://www.exforsys.com/tutorials/cloud-computing/cloud-computing-security.html)

Threat Model

- A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions
- Steps:
  - Identify attackers, assets, threats and other components
  - Rank the threats
  - Choose mitigation strategies
  - Build solutions based on the strategies

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Threat Model

- Basic components
  - Attacker modeling
    - Choose what attacker to consider
      - insider vs. outsider?
      - single vs. collaborator?
    - Attacker motivation and capabilities
  - Attacker goals
  - Vulnerabilities / threats

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

What is the issue?

- The core issue here is the levels of trust
  - Many cloud computing providers trust their customers
  - Each customer is physically commingling its data with data from anybody else using the cloud while logically and virtually you have your own space
  - The way that the cloud provider implements security is typically focused on the fact that those outside of their cloud are evil, and those inside are good.
- But what if those inside are also evil?

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Attacker Capability: Malicious Insiders

- At client
  - Learn passwords/authentication information
  - Gain control of the VMs
- At cloud provider
  - Log client communication
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns
  - Why?
    - Gain information about client data
    - Gain information on client behavior
    - Sell the information or use itself

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Attacker Capability: Outside attacker

- What?
  - Listen to network traffic (passive)
  - Insert malicious traffic (active)
  - Probe cloud structure (active)
  - Launch DoS
- Goal?
  - Intrusion
  - Network analysis
  - Man in the middle
  - Cartography

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Challenges for the attacker

- How to find out where the target is located?
- How to be co-located with the target in the same (physical) machine?
- How to gather information about the target?

From [5] www.cs.jhu.edu/~ragib/sp10/cs412

Part II: Security and Privacy Issues in Cloud Computing - Big Picture

- Infrastructure Security
- Data Security and Storage
- Identity and Access Management (IAM)
- Privacy

- And more…

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Infrastructure Security

- Network Level
- Host Level
- Application Level

The Network Level

- Ensuring confidentiality and integrity of your organization's data-in-transit to and from your public cloud provider
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider
- Ensuring availability of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers
- Replacing the established model of network zones and tiers with domains

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

The Network Level - Mitigation

- Note that network-level risks exist regardless of what aspects of "cloud computing" services are being used
- The primary determination of risk level is therefore not which *aaS is being used,
- But rather whether your organization intends to use or is using a public, private, or hybrid cloud.

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

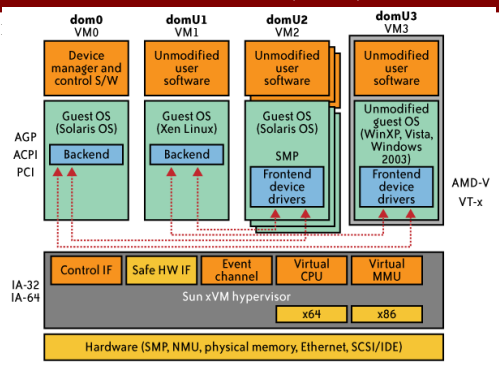
The Host Level

- SaaS/PaaS
  - Both the PaaS and SaaS platforms abstract and hide the host OS from end users
  - Host security responsibilities are transferred to the CSP (Cloud Service Provider)
    - You do not have to worry about protecting hosts
  - However, as a customer, you still own the risk of managing information hosted in the cloud services.

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

25

The Host Level (cont.)



From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Case study: Amazon's EC2 infrastructure

- "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds"
  - Multiple VMs of different organizations with virtual boundaries separating each VM can run within one physical server
  - "virtual machines" still have internet protocol, or IP, addresses, visible to anyone within the cloud.
  - VMs located on the same physical server tend to have IP addresses that are close to each other and are assigned at the same time
  - An attacker can set up lots of his own virtual machines, look at their IP addresses, and figure out which one shares the same physical resources as an intended target
  - Once the malicious virtual machine is placed on the same server as its target, it is possible to carefully monitor how access to resources fluctuates and thereby potentially glean sensitive information about the victim

27

Local Host Security

- Are local host machines part of the cloud infrastructure?
  - Outside the security perimeter
  - While cloud consumers worry about the security on the cloud provider's site, they may easily forget to harden their own machines
- The lack of security of local devices can
  - Provide a way for malicious services on the cloud to attack local networks through these terminal devices
  - Compromise the cloud and its resources for other users

28

Local Host Security (Cont.)

- With mobile devices, the threat may be even stronger
  - Users misplace or have the device stolen from them
  - Security mechanisms on handheld gadgets are often times insufficient compared to say, a desktop computer
  - Provides a potential attacker an easy avenue into a cloud system.
  - If a user relies mainly on a mobile device to access cloud data, the threat to availability is also increased as mobile devices malfunction or are lost
- Devices that access the cloud should have
  - Strong authentication mechanisms
  - Tamper-resistant mechanisms
  - Strong isolation between applications
  - Methods to trust the OS
  - Cryptographic functionality when traffic confidentiality is required

29

The Application Level

- DoS
- EDoS(Economic Denial of Sustainability)
  - An attack against the billing model that underlies the cost of providing a service with the goal of bankrupting the service itself.
- End user security
- Who is responsible for Web application security in the cloud?
- SaaS/PaaS/IaaS application security
- Customer-deployed application security

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

30

Data Security and Storage

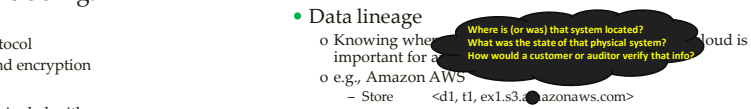
- Several aspects of data security, including:
  - Data-in-transit
    - Confidentiality + integrity using secured protocol
    - Confidentiality with non-secured protocol and encryption
  - Data-at-rest
    - Generally, not encrypted , since data is commingled with other users' data
    - Encryption if it is not associated with applications?
      - But how about indexing and searching?
      - Then homomorphic encryption vs. predicate encryption?
  - Processing of data, including multitenancy
    - For any application to process data, not encrypted

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

31

Data Security and Storage (cont.)

- Data lineage
  - Knowing whe… …oud is important for a…
  - e.g., Amazon AWS
    - Store <d1, t1, ex1.s3.…azonaws.com>
    - Process <d2, t2, ec2.co…pute2.amazonaws.com>
    - Restore <d3, t3, ex2.s3.amazonaws.com>



- Data provenance
  - Computational accuracy (as well as data integrity)
  - E.g., financial calculation: sum ((((2*3)*4)/6) -2) = $2.00 ?
    - Correct : assuming US dollar
    - How about dollars of different countries?
    - Correct exchange rate?

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

32

Data Security and Storage

- Data remanence
- Inadvertent disclosure of sensitive information is possible
- Data security mitigation?
- Do not place any sensitive data in a public cloud
- Encrypted data is placed into the cloud?
- Provider data and its security: storage
- To the extent that quantities of data from many companies are centralized, this collection can become an attractive target for criminals
- Moreover, the physical security of the data center and the trustworthiness of system administrators take on new importance.

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

33

Why IAM?

- Organization's trust boundary will become dynamic and will move beyond the control and will extend into the service provider domain.
- Managing access for diverse user populations (employees, contractors, partners, etc.)
- Increased demand for authentication
  - personal, financial, medical data will now be hosted in the cloud
  - S/W applications hosted in the cloud requires access control
- Need for higher-assurance authentication
  - authentication in the cloud may mean authentication outside F/W
  - Limits of password authentication
- Need for authentication from mobile devices

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

34

IAM considerations

Early this morning, at 3:30am PST, we started seeing elevated levels of authenticated requests from multiple users in one of our locations. While we carefully monitor our overall request volumes and these remained within normal ranges, we had not been monitoring the proportion of authenticated requests. Importantly, these cryptographic requests consume more resources per call than other request types.

Shortly before 4:00am PST, we began to see several other users significantly increase their volume of authenticated calls. The last of these pushed the authentication service over its maximum capacity before we could complete putting new capacity in place. In addition to processing authenticated requests, the authentication service also performs account validation on every request Amazon S3 handles. This caused Amazon S3 to be unable to process any requests in that location, beginning at 4:31am PST. By 6:48am PST, we had moved enough capacity online to resolve the issue.

As we said earlier today, though we're proud of our uptime track record over the past two years with this service, any amount of downtime is unacceptable. As part of the post mortem for this event, we have identified a set of short-term actions as well as longer term improvements. We are taking immediate action on the following: (a) improving our monitoring of the proportion of authenticated requests; (b) further increasing our authentication service capacity; and (c) adding additional defensive measures

35

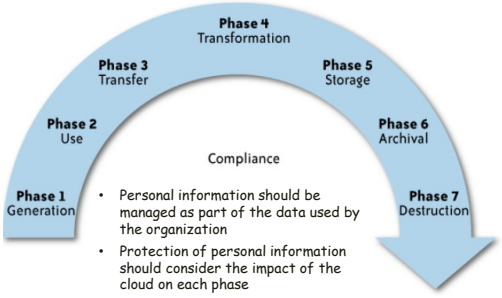
What is Privacy?

- The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions.
- It is shaped by public expectations and legal interpretations; as such, a concise definition is elusive if not impossible.
- Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data (or Personally Identifiable Information—PII).
- At the end of the day, privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization's practice around personal information.

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

36

What is the data life cycle?



From [6] Cloud Security and Privacy by Mather and Kumaraswamy

What Are the Key Privacy Concerns?

- Typically mix security and privacy
- Some considerations to be aware of:
  - Storage
  - Retention
  - Destruction
  - Auditing, monitoring and risk management
  - Privacy breaches
  - Who is responsible for protecting privacy?

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Storage

- Is it commingled with information from other organizations that use the same CSP?
- The aggregation of data raises new privacy issues
  - Some governments may decide to search through data without necessarily notifying the data owner, depending on where the data resides
- Whether the cloud provider itself has any right to see and access customer data?
- Some services today track user behaviour for a range of purposes, from sending targeted advertising to improving services

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Retention

- How long is personal information (that is transferred to the cloud) retained?
- Which retention policy governs the data?
- Does the organization own the data, or the CSP?
- Who enforces the retention policy in the cloud, and how are exceptions to this policy (such as litigation holds) managed?

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Destruction

- How does the cloud provider destroy PII at the end of the retention period?
- How do organizations ensure that their PII is destroyed by the CSP at the right point and is not available to other cloud users?
- Cloud storage providers usually replicate the data across multiple systems and sites—increased availability is one of the benefits they provide.
  - How do you know that the CSP didn't retain additional copies?
  - Did the CSP really destroy the data, or just make it inaccessible to the organization?
  - Is the CSP keeping the information longer than necessary so that it can mine the data for its own use?

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Auditing, monitoring and risk management

- How can organizations monitor their CSP and provide assurance to relevant stakeholders that privacy requirements are met when their PII is in the cloud?
- Are they regularly audited?
- What happens in the event of an incident?
- If business-critical processes are migrated to a cloud computing model, internal security processes need to evolve to allow multiple cloud providers to participate in those processes, as needed.
  - These include processes such as security monitoring, auditing, forensics, incident response, and business continuity

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Privacy breaches

- How do you know that a breach has occurred?
- How do you ensure that the CSP notifies you when a breach occurs?
- Who is responsible for managing the breach notification process (and costs associated with the process)?
- If contracts include liability for breaches resulting from negligence of the CSP?
  - How is the contract enforced?
  - How is it determined who is at fault?

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Who is responsible for protecting privacy?

- Data breaches have a cascading effect
- Full reli… data?
- In-… hip
- … data life cycle is…
- Many new risks and unknowns
  - The overall complexity of privacy protection in the cloud represents a bigger challenge.

e.g., Suppose a hacker breaks into Cloud Provider A and steals data from Company X. Assume that the compromised server also contained data from Companies Y and Z.

- **Who investigates this crime?**
- **Is it the Cloud Provider, even though Company X may fear that the provider will try to absolve itself from responsibility?**
- **Is it Company X and, if so, does it have the right to see other data on that server including logs that may show access to the data of Companies Y and Z?**

From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Part III. Possible Solutions

- Minimize Lack of Trust
  - Policy Language
  - Certification
- Minimize Loss of Control
  - Monitoring
  - Utilizing different clouds
  - Access control management
  - Identity Management (IDM)
- Minimize Multi-tenancy

References

1. NIST (Authors: P. Mell and T. Grance), "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology Laboratory (October 7 2009).
2. J. McDermott, (2009) "Security Requirements for Virtualization in Cloud Computing," presented at the ACSAC Cloud Security Workshop, Honolulu, Hawaii, USA, 2009.
3. J. Camp. (2001), "Trust and Risk in Internet Commerce," MIT Press
4. T. Ristenpart et al. (2009) "Hey You Get Off My Cloud," Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA
5. Security and Privacy in Cloud Computing, Dept. of CS at Johns Hopkins University. www.cs.jhu.edu/~ragib/sp10/cs412
6. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance by Tim Mather and Subra Kumaraswamy
7. Afraid of outside cloud attacks? You're missing the real threat. http://www.infoworld.com/d/cloud-computing/afraid-outside-cloud-attacks-youre-missing-real-threat-894
8. **Amazon downplays report highlighting vulnerabilities in its cloud service. http://www.computerworld.com/s/article/9140074/Amazon_downplays_report_highlighting_vulnerabilities_in_its_cloud_service**
9. **Targeted Attacks Possible in the Cloud, Researchers Warn.** http://www.cio.com/article/506136/Targeted_Attacks_Possible_in_the_Cloud_Researchers_Warn
10. **Vulnerability Seen in Amazon's Cloud-Computing by David Talbot.** http://www.cs.sunysb.edu/~sion/research/sion2009mitTR.pdf
11. **Cloud Computing Security Considerations by Roger Halbheer and Doug Cavit. January 2010.** http://blogs.technet.com/b/rhalbheer/archive/2010/01/30/cloud-security-paper-looking-for-feedback.aspx
12. **Security in Cloud Computing Overview.http://www.halbheer.info/security/2010/01/30/cloud-security-paper-looking-for-feedback**
13. **Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds by T. Ristenpart, E. Tromer, H. Shacham and Stefan Savage. CCS'09**
14. **Cloud Computing Security.** http://www.exforsys.com/tutorials/cloud-computing/cloud-computing-security.html
15. **Update From Amazon Regarding Friday's S3 Downtime by Allen Stern. Feb. 16, 2008.** http://www.centernetworks.com/amazon-s3-downtime-update
16. R. Ranchal, B. Bhargava, L.B. Othmane, L. Lilien, A. Kim, M. Kang, "Protection of Identity Information in Cloud Computing without Trusted Third Party," Third International Workshop on Dependable Network Computing and Mobile Systems (DNCMS) in conjunction with 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
17. P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Lilien, L.B. Othmane, "A User-Centric Approach for Privacy and Identity Management in Cloud Computing," 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
18. H. Khandelwal, *et al.*, "Cloud Monitoring Framework," Purdue University. Dec 2010.

Other References

- M. Armbrust, *et al.*, "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems LaboratoryFebruary 10 2009.
- Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing, ver. 2.1," 2009.
- M. Jensen, *et al.*, "On Technical Security Issues in Cloud Computing," presented at the 2009 IEEE International Conference on Cloud Computing, Bangalore, India 2009.
- P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm," ed: National Institute of Standards and Technology, Information Technology Laboratory, 2009.
- N. Santos, *et al.*, "Towards Trusted Cloud Computing," in *Usenix 09 Hot Cloud Workshop*, San Diego, CA, 2009.
- R. G. Lennon, *et al.*, "Best practices in cloud computing: designing for the cloud," presented at the Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications, Orlando, Florida, USA, 2009.
- P. Mell and T. Grance, "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology LaboratoryOctober 7 2009.
- C. Cachin, *et al.*, "Trusting the cloud," *SIGACT News*, vol. 40, pp. 81-86, 2009.
- J. Heiser and M. Nicolett, "Assessing the Security Risks of Cloud Computing," Gartner 2008.
- A. Joch. (2009, June 18) Cloud Computing: Is It Secure Enough? *Federal Computer Week*.
- AWS Amazon EC2: http://aws.amazon.com/ec2/
- Amazon CloudWatch: http://aws.amazon.com/cloudwatch/
- Iperf: http://iperf.sourceforge.net/